Samba on HP StorageWorks Enterprise File Services (EFS) Clustered File System Software

Installation and integration guide

PolyServe™

invent

Abstract

This guide describes steps to install and run Samba on HP StorageWorks Enterprise File Services (EFS) Clustered File System incorporating Samba failover support. The enclosed integration proof is designed to aid Professional Services in supporting similar installations in the field. This guide does not replace vendor installation documents or vendor customer support. These resources are assumed to exist before installation.

The software provided in the toolkit documented by this paper is provided as contributed software and is not a supported component of the HP Clustered File System Software.

Introduction

This document serves as a guideline for planning, installing, and managing Samba on HP StorageWorks EFS Clustered File System. As is the case with all software, changes to functionality, features, and form may obsolete information contained in this document. It is therefore advisable that the reader obtain the latest version of this document before proceeding.

This document is divided into the following sections:

- Application overview—Describes the application usage model and how the application is to be used in a psfs environment.
- Application configuration—Details the steps to configure the application for use with HP Clustered File System.
- For more information—References material that supports the use of HP Clustered File System and Samba.

Application overview

Samba is a suite of UNIX® applications that speak the Server Message Block (SMB) protocol. Many operating systems, including Microsoft® Windows® and OS/2, use SMB to perform client-server networking. By supporting this protocol, Samba allows UNIX servers to communicate with the same networking protocol as Microsoft Windows products. Thus, a Samba-enabled UNIX machine can masquerade as a server on your Microsoft network and offer the following services:

- Share one or more filesystems
- Share printers installed on both the server and its clients
- Assist clients with Network Neighborhood browsing
- Authenticate clients logging on to a Windows domain
- Provide or assist with WINS name server resolution

Today, the Samba suite revolves around a pair of UNIX daemons that provide shared resources—or shares—to SMB clients on the network. (Shares are sometimes called services as well.) These daemons are:

- smbd

  This daemon is responsible for managing the shared resources between the Samba server machine and its clients. It provides file, print, and browser services to SMB clients across one or more networks. smbd handles all notifications between the Samba server and the network clients. In addition, it is responsible for user authentication, resource locking, and data sharing through the SMB protocol.

- nmbd

  The nmbd daemon is a simple nameserver that mimics the WINS and NETBIOS name server functionality, as you might expect to encounter with the LAN Manager package. This daemon listens for nameserver requests and provides the appropriate information when called upon. It also provides browse lists for the Network Neighborhood and participates in browsing elections.

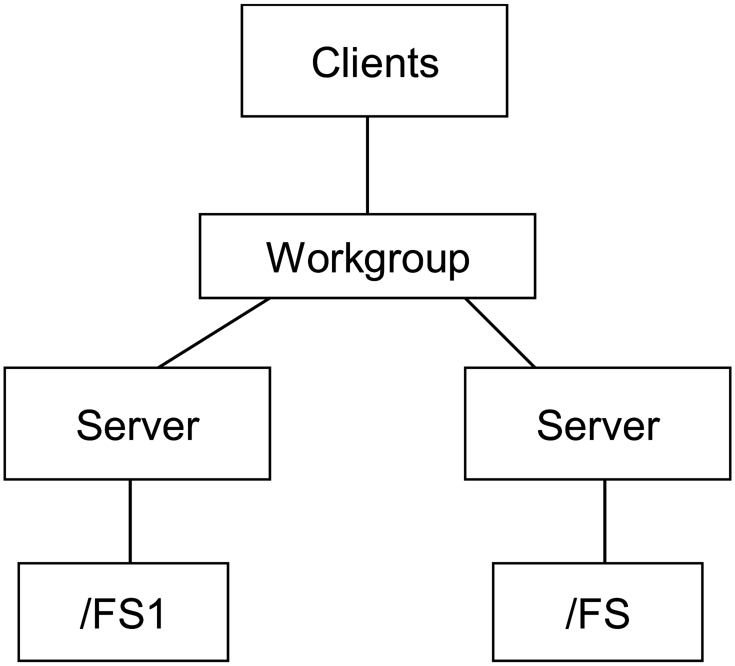
Microsoft has also contributed materially by putting forward its definition of SMB and the Internet savvy Common Internet File System (CIFS), as a public Request for Comments (RFC), a standards document. The CIFS protocol is Microsoft's renaming of future versions of the SMB protocol that will be used in Windows products—the two terms can be used interchangeably in this guide. Hence, you will often see the protocol written as "SMB/CIFS."

With any network access facility one should consider the security ramifications of providing such a service. This document discusses the basic security elements of CIFS, but does not cover in detail all the possible areas of security involving CIFS. It is assumed that the security requirements of each installation will be considered unique and will be handled on a case-by-case basis.

Samba has some basic concepts to be aware of for those who are not overly Microsoft Windows aware. From a hierarchical view the first item of interest is a workgroup, which is a logical grouping of clients that can share data from WINS servers, if configured to do so.

The next item of interest is the servers and client systems. In this usage, some of the servers listed are in fact virtual hosts, which can be moved from server to server in the cluster while keeping the same name. Lastly, under the server list is the name of the directory or what is more commonly known as shares.

Figure 1. Microsoft workgroup model



The value of using Samba on HP Clustered File System is that every server in the cluster can potentially host one or more psfs filesystems and fail them over to another server in the cluster. For example, there are four HP Clustered File System nodes all broadcasting themselves (NETBIOS name) as unique servers with each server responsible for a psfs filesystem. If the SMB clients attach by way of Samba only on the first node and that node crashes, access by all clients will be lost to the psfs filesystem, just like the traditional use of Samba on single server implementations.

The following discusses the HP Clustered File System using the same cluster configuration with the additional use of a virtual IP address and Samba virtual servers. All clients can use this virtual server as the host to attach the psfs filesystems. If the server supporting the virtual IP fails and moves to another server, the client connections would only have to reattach to the filesystem. Ideally, the ability to seamlessly move client connections from one server to another without reattaching would be preferable, but new server and client connections (session states) have to be re-established before operations can continue.

To accomplish this failover model in the vernacular of Samba, an abstraction technique called "virtual servers" is used. By manipulating the files that control virtual servers, a single system can appear as one or more virtual servers. Also, this virtual server can be moved to any configured server in the cluster.

Application configuration

The HP StorageWorks Enterprise File Services Clustered Gateway product has the standard Samba software pre-installed. However, the Samba failover scripts must be installed if they are to be used. It is not necessary to have Samba automatically started at this point since the following scripts will perform that task.

Note:
You must also configure the HP Clustered File System CLI for use on each node of the cluster. This procedure is described in the Command Reference guide. Without the proper installation and configuration, the deployment pack will not operate when creating the custom service monitor.

Samba server configuration

In the dist-samba_d.tar.gz toolkit (found in the /opt/hpcfs/contrib directory) are all the necessary scripts and template scripts to configure each cluster member for virtual server failover. To install the toolkit, perform the following steps:

```
% cd /opt/hpcfs/contrib
% tar xzf dist-samba_d.tar.gz
% cd SAMBA
% make install
```

Samba configuration file: /etc/samba/smb.default

This file contains the workgroup and the netbios name of the server that Samba is running on. It is to be identical on each cluster member.

```
# smb.conf
# Global parameters
[global]
   netbios name = %h
   workgroup = HP ←———— Needs to be assigned
```

If workgroup is not assigned, the default for Samba is WORKGROUP, which is not recommended.

The %h returns the Internet name of the host from NIS, DNS, or /etc/hosts. The workgroup is the name of the network.

This configuration, if started as is, would broadcast the server (hostname) and allow only login access with no visible shares available.

Samba configuration file: /etc/samba/smb.conf.<Samba Virtual Server>

This file contains the specifics about the share name that you want to broadcast from this server. These files are identically configured on all cluster servers with the exception of the **interfaces** and **socket address.** Two example configuration files are listed.

Smb.conf has many different options for defining characteristics about the share, which goes beyond the scope of this document. For mixed encryption and plaintext password clients, you can describe two shares with unique names for the same directory, with one having encryption turned on and the other turned off.

```
# Global parameters for smb.conf.sharename
                           ^
                    Virtual Server
[global]
   interfaces = 192.168.1.111/24
   socket address = 192.168.1.111
   ;encrypt passwords = Yes                        # Only uncomment if using encryption
   ;smb passwd file = /etc/samba/smbpasswd         # Only uncomment if using encryption
   log file = /var/log/samba/%m.log
   max log size = 0
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   dns proxy = No
   local master = yes
   preferred master = yes

[/cifsdata directory]
   comment = /cifsdata Directory on %h
   path = /cifsdata
   valid users = someuser
   writeable = Yes
```

The configuration file smb.conf has many different options for defining characteristics about the share, which goes beyond the scope of this document. For mixed encryption and plaintext password clients, you can describe two shares with unique names for the same directory, with one having encryption turned on and the other turned off.

To set each Samba user's password, use the command smbpasswd –a **username** (replace username with each user's username). A Samba user account will not be active until a Samba password is set for it.

Migrate the Samba configuration files

After you have completed configuring the Samba deployment kit files, migrate the changed files to all other servers in the cluster in "/etc/samba."

Failover configuration

In addition to the Samba configuration files previously mentioned, Samba virtual server failover is accomplished with the use of a **custom service monitor** script that will be used by HP Clustered File System to fail over virtual servers. The script is called smb_meth and is part of the toolkit. The script is installed by the deployment kit and is located in /opt/hpcfs/methods.

- Failover considerations

  The deployment pack also gives users the ability to determine if they want a cifs share to fail over and stay or fail back as soon as the previous server it was running on rejoins the cluster. The benefit of fail and stay is that you eliminate the need to fail back (another service interruption) and when the previous server that supported the cifs share rejoins the cluster, it can now be a backup for the cifs share. By default this ability is turned off, so cifs shares automatically fail back. To enable it, simply add **–f Y** to the commandline arguments when creating your custom service monitor, as shown in the following example. If this is not the behavior you want, omit the arguments.

- Virtual server and share associations

  Next you will need to determine the relationship of virtual servers to file shares. The only usage model that is supported is an active/passive model with a unique psfs filesystem only available from one server at a time. You can fail over the virtual server/file share to another server that is currently broadcasting a different virtual share/file share.

Service monitor configuration

Using a two-node example, first create two virtual hosts with one primary to each system. The share name that represents both /data1 and /data2 will be SH.

VH = virtual host	VH1= 192.168.1.111	VH2=192.168.1.121
/etc/host entries	192.168.1.111 cifsshare1	192.168.1.121 cifsshare2

When entering IP addresses in the interface line you will notice the use of /24 (CIDR format). It represents the netmask, for example, /24 is class C, /16 is class B, and /8 is class A. Netmask can be represented in full dot form as well. The following demonstrates this configuration.

These two smb.conf.<cifsshare name> files live on both servers.

smb.conf.cifsshare1

```
Global parameters for smb.conf.cifsshare1
[global]
    interfaces = 192.168.1.111/24
    socket address = 192.168.1.111
    ;encrypt passwords = Yes
    ;smb passwd file = /etc/samba/smbpasswd
    log file = /var/log/samba/%m.log
   max log size = 0
   socket options = TCP_NODELAY SO_RCVBUF=8192
   SO_SNDBUF=8192
   dns proxy = No

[ cifsdata1]

   comment = /data1 Directory on %h
   path = /data1
   writeable = Yes

[ cifsdata2]

   comment = /data2 Directory on %h
   path = /data2
   writeable = Yes
```

smb.conf.cifsshare2

```
# Global parameters for smb.conf.cifsshare2
[global]
   interfaces = 192.168.1.121/24
   socket address = 192.168.1.121
   ;encrypt passwords = Yes
   ;smb passwd file = /etc/samba/smbpasswd
   log file = /var/log/samba/%m.log
   max log size = 0
   socket options = TCP_NODELAY SO_RCVBUF=8192
   SO_SNDBUF=8192
   dns proxy = No

[ cifsdata3]

   comment = /data3 Directory on %h
   path = /data3
   writeable = Yes

[ cifsdata4]

   comment = /data4 Directory on %h
   path = /data4
   writeable = Yes
```

Additional parameters can be added or deleted from this file with the exception of the **interfaces** and **socket address** line. Some more applicable ones can be found in the supporting documentations section.

Select the server and its virtual host (primary) that represents where you want the share “cifsshare1” to run normally. From the GUI, create a Custom Service Monitor. Name the service the cifs share name (cifsshare1 or cifsshare2). You can use default timeout of 120 seconds and a 60-second probe frequency.

For the probe, start and stop scripts use the following (using cifsshare1 in this example):

Probe: `/opt/hpcfs/methods/smb_meth –f Y cifsdata1`

Start: `/opt/hpcfs/methods/smb_meth –f Y cifsdata1 Timeout =300`

Stop: `/opt/hpcfs/methods/smb_meth –f Y cifsdata1 Timeout =300`

The Service Monitor for cifsshare1 supporting the disk shares cifsdata1 and cifsdata2 will start on the vhost primary.

For more information

References

- http://www.samba.org
- http://us1.samba.org/samba/docs/

Using Samba

O'Reilly and Associates, Inc

Robert Eckstein, David Collier-Brown, and Peter Kelly

January 2000 First Edition

David Collier-Brown

Performance & Engineering

Americas Customer Engineering

Sun, Inc. Canada

Personal response to a posting on "Re: Error in Using Samba, chapter 4, on Virtual Servers"

Last known location: http://lists.samba.org/archive/samba-technical/2000-August/009304.html

Howtos

http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/

4AA0-0945ENW, 07/2005